

CLAIMS

1. An electronic cash system comprising an electronic cash management apparatus, a settlement apparatus, and a management apparatus, for processing a payment to an amount due with previously deposited funds, said electronic cash system characterized in that:

said electronic cash management apparatus includes:

storage means for storing information for identifying a user, and the amount of money utilized by said user based on the previously deposited funds;

said settlement apparatus includes:

settlement instructing means for instructing a payment institution to settle;

said management apparatus includes:

management means for managing said information for identifying a user, and an account number in the payment institution of the user, encrypted with a public key of said settlement apparatus;

balance change instructing means for instructing said electronic cash management apparatus to change the balance of the deposited funds of said user, stored in said storage means of said electronic cash management apparatus, based on said information for identifying a user managed by said management means; and

settlement execution instructing means for instructing said settlement instructing means of said settlement processing apparatus to execute a settlement based on the account number in said payment

institution managed by said management means.

2. An electronic cash system according to claim 1, wherein:
said electronic cash management apparatus, said settlement apparatus and said management apparatus perform predetermined mutual authentication processing before communications.
3. An electronic cash system according to claim 1, wherein:
data transmitted between said electronic cash management apparatus, said settlement apparatus and said management apparatus is encrypted.
4. An electronic cash storing method for previously depositing funds for possible payments in an information processing apparatus, characterized by:
mutually authenticating with a management apparatus, and sharing a temporary key therewith;
said information processing apparatus encrypting an issued amount to be deposited with said temporary key, encrypting a credit card number with a public key of a settlement apparatus, and transmitting said issued amount and said credit card number to said management apparatus;
said management apparatus receiving said issued amount and said credit card number, decrypting said issued amount with said temporary key, and transmitting said encrypted credit card number and said issued amount to said settlement apparatus;

said settlement apparatus decrypting said credit card number received thereby with a secret key of said settlement apparatus, and performing a settlement based on said decrypted credit card number and said issued amount; and

said management apparatus transmitting said issued amount to an electronic cash management apparatus, and said electronic cash management apparatus storing said issued amount together with a device number unique to each said information processing apparatus.

5. An electronic cash storing method for previously depositing funds for possible payments in an information processing apparatus, characterized by:

mutually authenticating with a management apparatus, and sharing a temporary key therewith;

said information processing apparatus encrypting an issued amount to be deposited and a device number unique to each said information processing apparatus with said temporary key, and transmitting the same to said management apparatus;

said management apparatus decrypting said issued amount and said unique number received thereby with said temporary key, finding a credit card number encrypted with a public key of a settlement apparatus corresponding to said device number from a storage device, and transmitting said encrypted credit card number and said issued amount to said settlement apparatus;

said settlement apparatus decrypting said credit card number

received thereby with a secret key of said settlement apparatus, and performing a settlement based on said decrypted credit card number and said issued amount; and

said management apparatus also transmitting said device number and said issued amount to said electronic cash management apparatus, and said electronic cash management apparatus storing said unique number and said issued amount.

6. A method of transferring electronic cash from an information processing apparatus 2 to an information processing apparatus 1, characterized by:

said information processing apparatus 1 and said information processing apparatus 2 mutually authenticating with each other, and sharing a temporary key therebetween;

said information processing apparatus 2 encrypting a amount to be transferred, appended with a signature of said information processing apparatus 2, with said temporary key, and transmitting the same to said information processing apparatus 1;

said information processing apparatus 1 decrypting said amount received thereby with said temporary key, and adding said amount to an amount previously held by said information processing apparatus 1;

said information processing apparatus 1 encrypting said amount appended with a signature of said information processing apparatus 1 with said temporary key, and transmitting the same to said information processing apparatus 2; and

said information processing apparatus 2 decrypting said amount received thereby with said temporary key, and subtracting said amount from an amount previously held by said information processing apparatus 2.

7. An electronic cash transfer method according to claim 6, wherein:
said information processing apparatus 2 transmits the amount to be transferred together with a device number unique to said information processing apparatus 2 encrypted with a public key of a management apparatus, to said information processing apparatus 1.

8. An electronic cash system comprising an information processing apparatus, a shop, an electronic cash management apparatus, a settlement apparatus, and a management apparatus, adapted to processing a payment to an amount due with previously deposited funds, characterized by:

said information processing apparatus transmitting to said shop, information on an article to be purchased, a number unique to said information processing apparatus encrypted with a public key of said management apparatus, and transmitting a payment for said purchased article encrypted with a public key of said electronic cash management apparatus;

said shop confirming said information on the article to be purchased, received thereby, and transmitting said number unique to said information processing apparatus and a proceed for said purchased article to said management apparatus;

said management apparatus decrypting said encrypted number unique to said information processing apparatus, received thereby, with a secret key of said management apparatus, and transmitting said number unique to said information processing apparatus and said proceed for the purchased article to said cash management apparatus;

said cash management apparatus decrypting said encrypted proceed for the purchased article, received thereby, with a secret key of said cash management apparatus, and storing the same together with said number unique to said information processing apparatus; and

after a normal completion of said processing, said information processing apparatus subtracting said payment for the purchased article from electronic cash previously held thereby, and recording the resulting electronic cash.